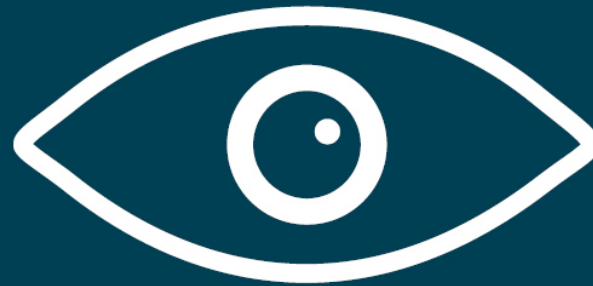


САРЧАРТО
ДОРАРАРТЧ



**Ich will nicht in einer Welt leben,
in der alles, was ich sage, alles was ich mache,
der Name jedes Gesprächspartners,
jeder Ausdruck von Kreativität,
Liebe oder Freundschaft aufgezeichnet wird.**

Edward Snowden

Digitalcourage e.V.

- Gemeinnütziger Verein für Datenschutz und Bürgerrechte
 - "Für eine lebenswerte Welt im digitalen Zeitalter"
 - Big Brother Awards
 - Aktionen zu aktuellen Themen
- Digitalcourage Hochschulgruppe
 - Cryptopartys
 - Backup-Partys
 - Linux-Install-Partys
 - Regelmäßige Treffen an der Uni

Agenda

- Inputvortrag zu:
 - Windows 10
 - Sichere Passwörter
 - Verschlüsselung von E-Mails (PGP)
 - Festplatten-/Dateiverschlüsselung
 - Sicheres Surfen mit Privatsphäre & Tor
 - Mobilgeräte
- Praxis

"Datenschutzalbtraum" Windows 10

"Datenschutzalbtraum" Windows 10?

- Windows-Store mit zahlreichen vorinstallierten Apps
 - z.B. Cloud-Dienst "OneDrive" oder Browser und PDF-Reader "Edge"
- "Sprachassistentin" Cortana
- Systemupgrades, die nur aufgeschoben werden können

Kunde als Ware?!

- "Microsoft erhebt **Daten**, um **effektiv arbeiten** und Ihnen die **besten Erfahrungen mit unseren Produkten** anbieten zu können. Sie stellen einige dieser Daten direkt bereit, beispielsweise wenn Sie ein **Microsoft-Konto erstellen**, eine **Suchanfrage** bei Bing einreichen, einen **Sprachbefehl** an Cortana erteilen, [... können wir] Ihre Interaktion mit unseren Produkten aufzeichnen [...] Wir erhalten ebenfalls Daten von Drittanbietern."

<https://privacy.microsoft.com/de-de/privacystatement>

- **Zweck der Sammelwut: mit den Daten der eigenen Kunden Geld verdienen!**
- Quelle: Datenschutzerklärung Win10

Startseite

Einstellung suchen

Datenschutz

- Allgemein
- Position
- Kamera
- Mikrofon
- Benachrichtigungen
- Spracherkennung, Freihand und Eingab
- Kontoinformationen
- Kontakte
- Kalender
- Anrufliste
- E-Mail

Einige Einstellungen werden von Ihrer Organisation verwaltet.

Datenschutzooptionen ändern

Apps die Verwendung der Werbe-ID für App-übergreifende Erlebnisse erlauben (bei Deaktivierung wird Ihre ID zurückgesetzt)

☐ Aus

SmartScreen-Filter einschalten, um von Windows Store-Apps verwendete Webinhalte (URLs) zu überprüfen

☐ Aus

Informationen zu meinem Schreibverhalten an Microsoft senden, um die Eingabe- und Schreibfunktionen in Zukunft zu verbessern

☐ Aus

Websites den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen

☐ Aus

Apps auf anderen Geräten das Öffnen von Apps gestatten und auf der Oberfläche dieses Geräts weiterarbeiten

☐ Aus

Apps auf anderen Geräten das Öffnen von Apps über Bluetooth gestatten und auf der Oberfläche dieses Geräts weiterarbeiten

☐ Aus

Microsoft-Werbung und andere Personalisierungsinfos verwalten

Microsoft-Konto und sonstige „Cloud“-Daten, z.B. Office 365, Outlook

Startseite

Einstellung suchen

Datenschutz

Kalender

Anrufliste

E-Mail

Messaging

Funkempfang

Weitere Geräte

Feedback und Diagnose

Hintergrund-Apps

Feedbackhäufigkeit

Mein Feedback soll von Windows angefordert werden

Nie

[Geben Sie uns Feedback zu Umfragebenachrichtigungen von Feedback-Hub.](#)

Diagnose- und Nutzungsdaten

Sendet Ihre Gerätedaten an Microsoft.

Einfach

Verbessert

Vollständig (empfohlen)

gesendet werden.

**Fehlt: Keine
Daten senden**

dem Umfang Windows-
Gerät an Microsoft

[Weitere Informationen zu Feedback- und Diagnoseeinstellungen](#)

[Datenschutzbestimmungen](#)

Diagnose- und Nutzungsdaten = Vollständig

- Bei der **Einstellung "Vollständig"** sendet Win10 u.a. die folgenden Daten an Microsoft:
 - Daten über App-Verwendung (z.B. welche Apps, Nutzungsdauer und Reaktionszeit)
 - Browser-Nutzung, einschließlich Browserverlauf und Suchbegriffe
 - Teilweise Freihand- und Tastatureingaben (lt. Microsoft werden alle personenbezogenen Daten entfernt)
 - "Erweiterte Fehlerberichterstattung, die den Speicherstatus des Geräts bei einem System- oder App-Absturz umfasst. Dabei können unbeabsichtigt Teile der Datei übermittelt werden, die Sie beim Auftreten des Problems verwendet haben."
 - Datenweitergabe an OEM-Partner (z.B. Fehlerberichte)

Schutz gegen den "Datenschutzalbtraum"

- Was könnt Ihr dagegen tun?
- Keine Tools oder 1-Click-Lösungen (z.B. O&O ShutUp10, DoNotSpy10)
- Einfach und nutzerfreundlich
 - Paper vom AKIF – Orientierungshilfe zur datenarmen Konfiguration von Windows 10, abrufbar unter: https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf
- Übergangslösung: So lang wie möglich bei einer älteren Windows-Version bleiben
- Auf Linux umsteigen; Windows nur noch für Programme nutzen, die unter Linux nicht laufen

Fazit

- **"However, there is still no extensive guidance on how Windows 10 can be used in full compliance with European data protection law.",**
- Bayrisches Landesamt für Datenschutz
- Quelle: https://www.lida.bayern.de/media/windows_10_report.pdf

Literaturempfehlung

- Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen (AKIF) der Max-Planck-Gesellschaft, Orientierungshilfe zur datenarmen Konfiguration von Windows 10; Stand: 06.12.2016; abrufbar unter:
https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf
- Mike Kuketz, Windows 10: Dem Kontrollverlust entgegenwirken; Stand: 28. März 2017; abrufbar unter
<https://www.kuketz-blog.de/windows-10-dem-kontrollverlust-entgegenwirken/>
- Datenschutzerklärung von Microsoft; Stand: März 2017; abrufbar unter
<https://privacy.microsoft.com/de-de/privacystatement>
- Mehr zu Linux; Stand: Dezember 2017:

Die vier Freiheiten der Freien Software

- 1) Uneingeschränktes Verwenden zu jedem Zweck.
- 2) Das Recht, die Funktionsweise zu untersuchen und zu verstehen.
- 3) Das Recht, Kopien der Software zu verbreiten.
- 4) Das Recht, die Software zu verbessern und die Verbesserungen zu verbreiten.

Sichere Passwörter

Wie werden Passwörter geknackt?

- Brute Force
 - Alle möglichen Kombinationen ausprobieren
- Listen / Wörterbuch-Angriffe
 - Alle Wörter aus einer Liste oder einem Wörterbuch ausprobieren
- Social Engineering
 - Phishing, Person austricksen um PW zu erfahren
 - Gerne auch durch Facebook, LinkedIn etc.

Wie erschwert man das Knacken des Passwords?

- Brute Force
 - ⇒ Länge (10+ Zeichen)
 - ⇒ Verschiedene Zeichentypen
(Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)

Wie erschwert man das Knacken des Passwords?

- Brute Force
 - ⇒ Länge (10+ Zeichen)
 - ⇒ Verschiedene Zeichentypen
(Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)
- Listen / Wörterbuch-Angriffe
 - ⇒ Kein einzelnes Wort als PW verwenden
 - ⇒ Keine Wörter aus dem Umfeld (Namen, Geburtsdaten)

Wie erschwert man das Knacken des Passwords?

- Brute Force
 - ⇒ Länge (10+ Zeichen)
 - ⇒ Verschiedene Zeichentypen
(Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)
- Listen / Wörterbuch-Angriffe
 - ⇒ Kein einzelnes Wort als PW verwenden
 - ⇒ Keine Wörter aus dem Umfeld (Namen, Geburtsdaten)
- Social Engineering
 - ⇒ Niemandem das Passwort verraten!

Sichere Passwörter finden

- Wichtig:
 - Für jeden Dienst ein anderes Passwort verwenden!
 - Passwörter in regelmäßigen Abständen austauschen/ändern
- DBiR&dSd90M!
 - Merksatz: »**Der Ball ist Rund & das Spiel dauert 90 Minuten!**«
- AliensHexenHotelGemahlin
 - Wortreihung (min. 4 **zufällige** Wörter)
- 2UrN47oCfK6jAZ8xuKHioP4upPsl73
 - Passwortgenerator

Passwortverwaltung

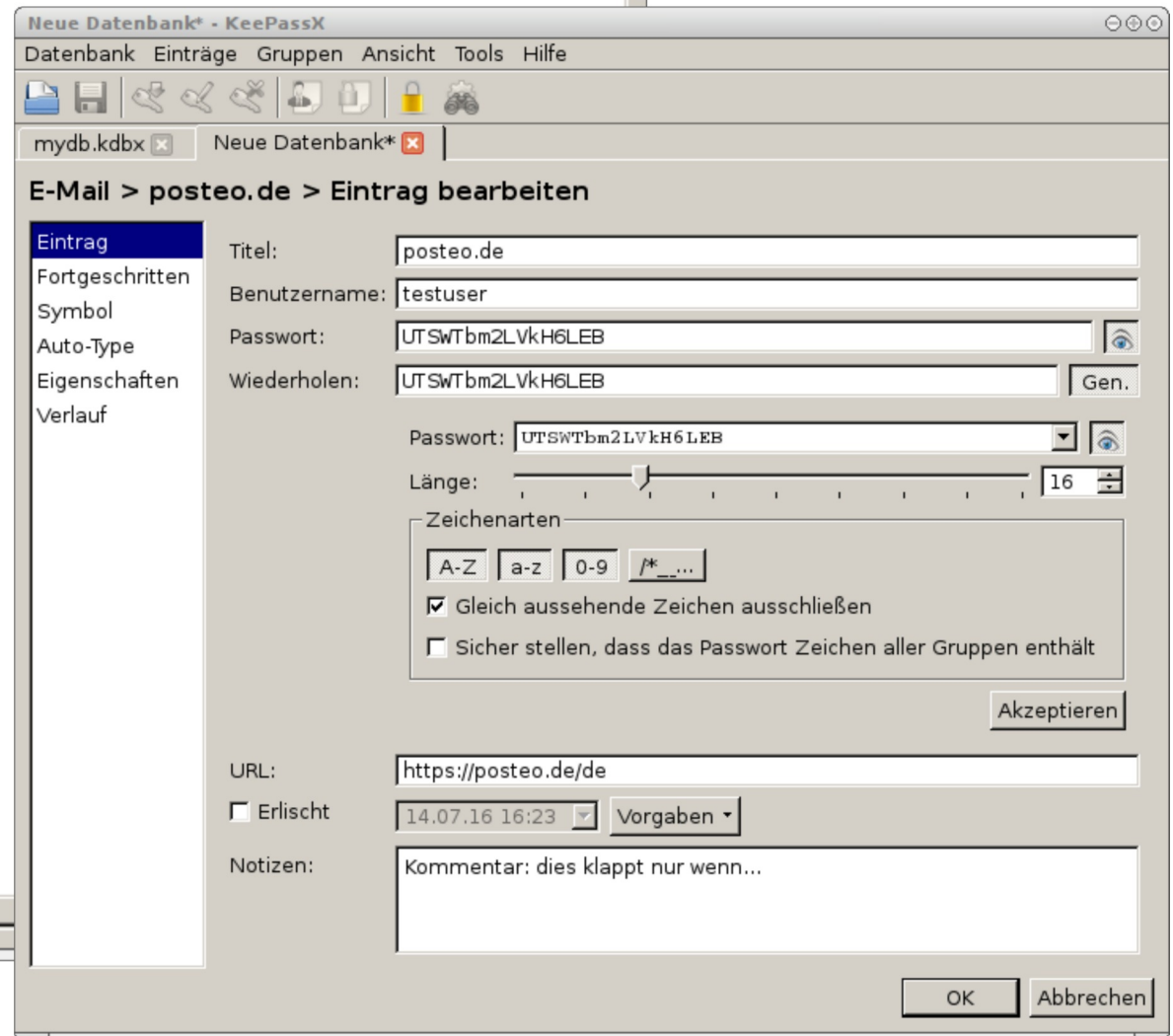
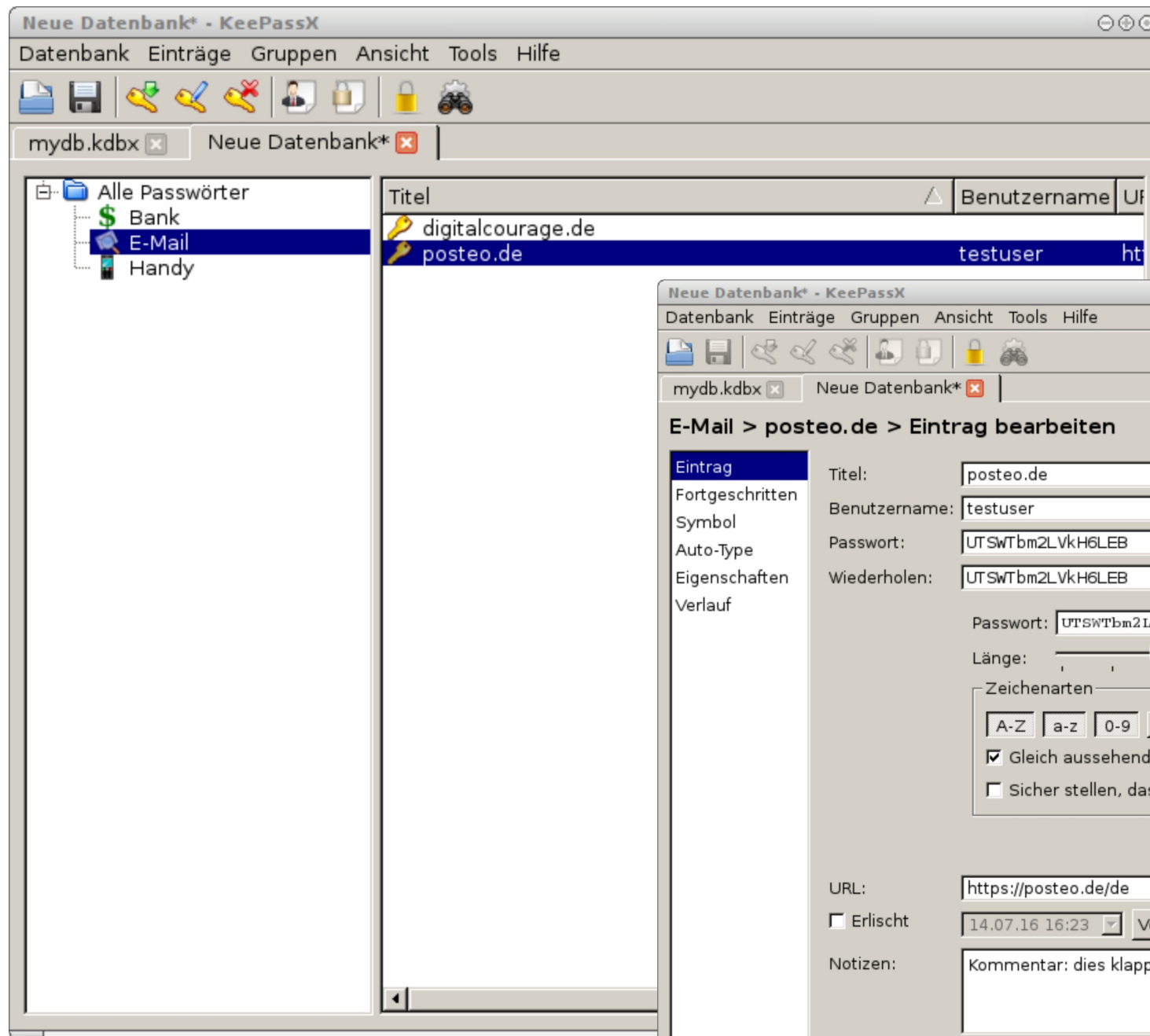
Software: **KeePassX**

Vorteile

- Freie Software
- Viele Plattformen
 - Win, Linux, Mac, Android
- Passwortgenerator
- Verschlüsselt gespeichert

Nachteile

- Masterpasswort
 - Darf nicht vergessen oder geknackt werden!
- Gefahr bei Verlust
 - „Setzt alles auf eine Karte“:
PW-Datenbank gut sichern!
- Komfort
 - Kein Sync zwischen verschiedenen Geräten



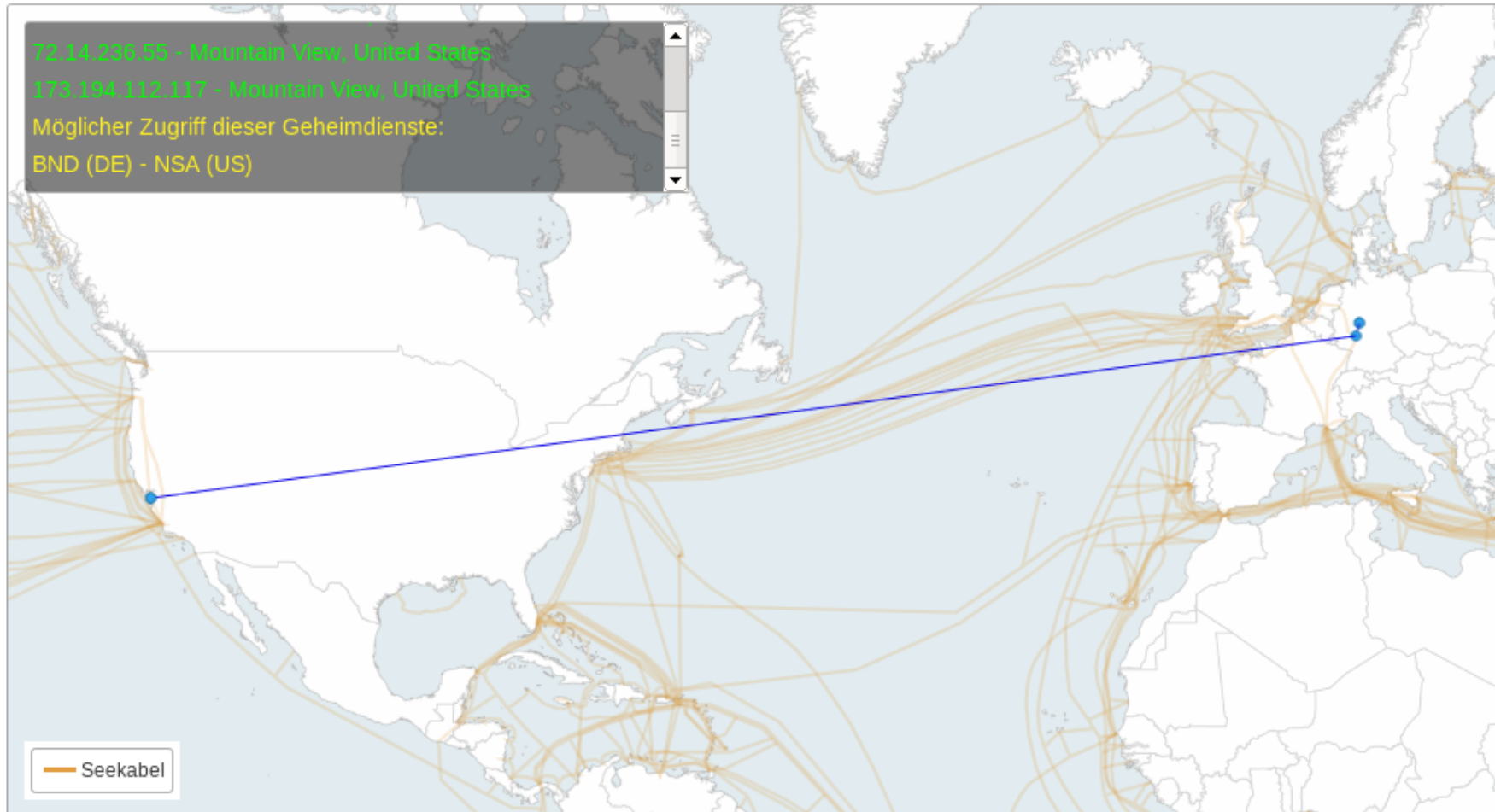
Videoempfehlung

- Um das eben erklärte zu wiederholen, seht Euch bitte das Video von Alexander Lehmann " Passwörter Einfach Erklärt" an; abrufbar unter: <https://vimeo.com/138839266>

E-Mail-Verschlüsselung

E-Mail Anbieter

Anfragen aus **Deutschland** / der Schweiz / Frankreich



Quelle: <http://apps.opendatacity.de/prism/de>

Alternativen zu „kostenlosen“ E-Mail-Anbietern

- **Posteo.de** oder **mailbox.org**
- 24h-Einmal-E-Mail-Adresse, gratis: anonbox.net (CA-Cert)

Vorteile

- Standort in Deutschland
- Datensparsamkeit
- Keine Inhaltsanalyse
- Keine Werbung
- Anonyme Nutzung möglich
- Datenschutz hat Priorität

Nachteile

- **posteo.de** und **mailbox.org**
kosten 1 € pro Monat

E-Mail-Verwaltung

- Software: **Mozilla Thunderbird**
 - Freie Software
 - Mehrere Mail-Konten möglich
 - Verwaltung mit Filtern und Ordnern
 - HTML abschalten möglich
 - Mails offline lesen, speichern und durchsuchen
 - Add-ons: Kalender, Massenmails, **Verschlüsselung**

Posteingang - test1@digitalcourage.de - Icedove

Posteingang - test1@di...

Abrufen

Verfassen

Chat

Adressbuch

Schlagwörter

Schnellfilter

Suchen... <Strg+K>

test1@digitalcourage.de

Posteingang

cryptoseminiare

digitalcourage

Mailingliste1 (1)

Mailingliste2

test

Gesendet

Papierkorb

test2@digitalcourage.de

Posteingang (1)

Gesendet

Papierkorb

test3@digitalcourage.de

Posteingang (2)

Mailingliste1

Papierkorb

Lokale Ordner

Papierkorb

Postausgang

Archivierte Mails

	Betreff	Von	Datum	Größe
☆	Willkommen	georg test	15:47	0,9 KB
☆	Ich bin weg...	test2@digitalcourage....	15:48	1,0 KB

Antworten

Weiterleiten

Archivieren

Junk

Löschen

Mehr

Von Mir <test2@digitalcourage.de> ☆

Betreff **Ich bin weg...** 15:48

An Mich <test1@digitalcourage.de> ☆

Ich bin vom <date> bis <date> nicht zu Hause / im Büro.
 In dringenden Fällen setzen Sie sich bitte mit <contact person> in Verbindung.
 Vielen Dank für Ihr Verständnis.

Ungelesen: 0

Gesamt: 2

▶ digitalcourage

28 / 81

E-Mail-Verschlüsselung (PGP)

Vorteile

- Inhalt Ende-zu-Ende-verschlüsselt
- Absender¹ & Empfängerin werden eindeutig (¹ mit PGP-Signatur)

Nachteile

- Metadaten (von, an, Betreff etc). bleiben unverschlüsselt
- Absender & Empfängerin müssen PGP nutzen

Benötigte Software:

- E-Mail Programm: Thunderbird
- Add-on: **Enigmail**

Unterschied symmetrische / asymmetrische Verschlüsselung

Symmetrische Verschlüsselung

- Wie analoge Schlüssel
- **Derselbe Schlüssel** zum Ver- und Entschlüsseln
- Alle Beteiligten brauchen diesen (geheimen) Schlüssel
- Problem: um Nachrichten (auf unsicheren Kanälen) zu senden, muss zuerst der Schlüssel (auf sicherem Kanal) verteilt werden

Unterschied symmetrische / asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung → PGP

- **Schlüsselpaar:** was **ein** Schlüssel **verschlüsselt**, muss mit dem **anderen** Schlüssel **entschlüsselt** werden
- Alle Beteiligten erzeugen ein eigenes Schlüsselpaar
- Öffentlicher Schlüssel (zum Verschlüsseln)
 - kann und muss verteilt werden (an alle, über unsichere Kanäle)
- Privater Schlüssel (zum Entschlüsseln)
 - bleibt privat – gut schützen und sichern, niemals herausgeben!

Unterschied symmetrische / asymmetrische Verschlüsselung

- Es gilt:
 - Absender braucht **öffentlichen Schlüssel der Empfängerin**
 - nur Empfängerin kann (mit ihrem privaten Schlüssel) entschlüsseln

PGP Public Keys austauschen

- E-Mail Anhang
 - .asc Datei
- Key-Server
 - Bequem durchsuchbar
 - E-Mail-Adresse öffentlich einsehbar

Digitale Signatur mit PGP

- Analoger Vergleich: Siegel
 - Sender eindeutig: Authentizität
 - Nachricht nicht manipuliert: Integrität
- Auch ohne Verschlüsseln möglich
- Beispiel:

```
-----BEGIN PGP SIGNATURE-----  
iQA/AwUBONpOg40d+PaAQUTIEQIc5ACdGkKSzpOrsT0Gvj  
3jH9NXD8ZP2IcAn0vj/BHT+qQCtPCtCwO1aQ3Xk/NL=1CZt  
-----END PGP SIGNATURE-----
```

Schlüssel-Fingerabdruck

- Echtheit von öffentlichen Schlüsseln überprüfen
- Eine Art "Quersumme"
- Weltweit nur auf einen Schlüssel passend
- Beispiel:
 - Fingerprint zum öffentlichen Schlüssel mit der ID 0x315DFB0A
 - DF31 49DD 7046 0F3A 7F17 3C4A 4818 84B5 315D FB0A

Posteingang - test1@digitalcourage.de - Icedove

Posteingang - test1@di...

Abrufen ▾ | Verfassen | Chat | Adressbuch | Schlagwörter ▾ | Schnellfilter | Suchen... <Strg+K>

test1@digitalcourage.de

- Posteingang
 - cryptoseminiare
 - digitalcourage
 - Mailingliste1 (1)
 - Mailingliste2
 - test
 - Gesendet
 - Papierkorb
- test2@digitalcourage.de
 - Posteingang (1)
 - Gesendet
 - Papierkorb
- test3@digitalcourage.de
 - Posteingang (2)
 - Mailingliste1
 - Papierkorb
- Lokale Ordner
 - Papierkorb
 - Postausgang
 - Archivierte Mails

	Betreff	Von	Datum	Größe
☆	Willkommen	georg test	15:47	0,9 KB
☆	Ich bin weg...	test2@digitalcourage....	15:48	1,0 KB

Verfassen: verschlüsselte Mail

Datei Bearbeiten Ansicht Optionen Enigmail Extras Hilfe

Senden | Rechtschr. ▾ | Anhang ▾ | S/MIME ▾ | Speichern ▾

Enigmail: Meinen öffentlichen Schlüssel anhängen | Nachricht wird unterschrieben und verschlüsselt.

Von: georg test <test1@digitalcourage.de> test1@digitalcourage.de

An: test3@digitalcourage.de

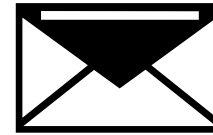
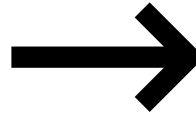
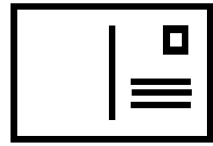
An:

Betreff: verschlüsselte Mail

Hallo Test3,

endlich habe ich mir Verschlüsselung eingerichtet ...

Ungelesen: 0 Gesamt: 2



"Privacy is the right to a free mind."

– Edward Snowden

Dateiverschlüsselung

Warum überhaupt verschlüsseln?

- Genereller Schutz sensibler und vertraulicher Daten
 - Bei Verlust/Diebstahl des Laptops oder USB-Stick
 - Jeder der personenbezogene Daten speichert
- Weil Ihr ein Grundrecht auf digitale Intimsphäre habt!
 - Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
 - sog. IT-Grundrecht, Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG

Dateiverschlüsselung

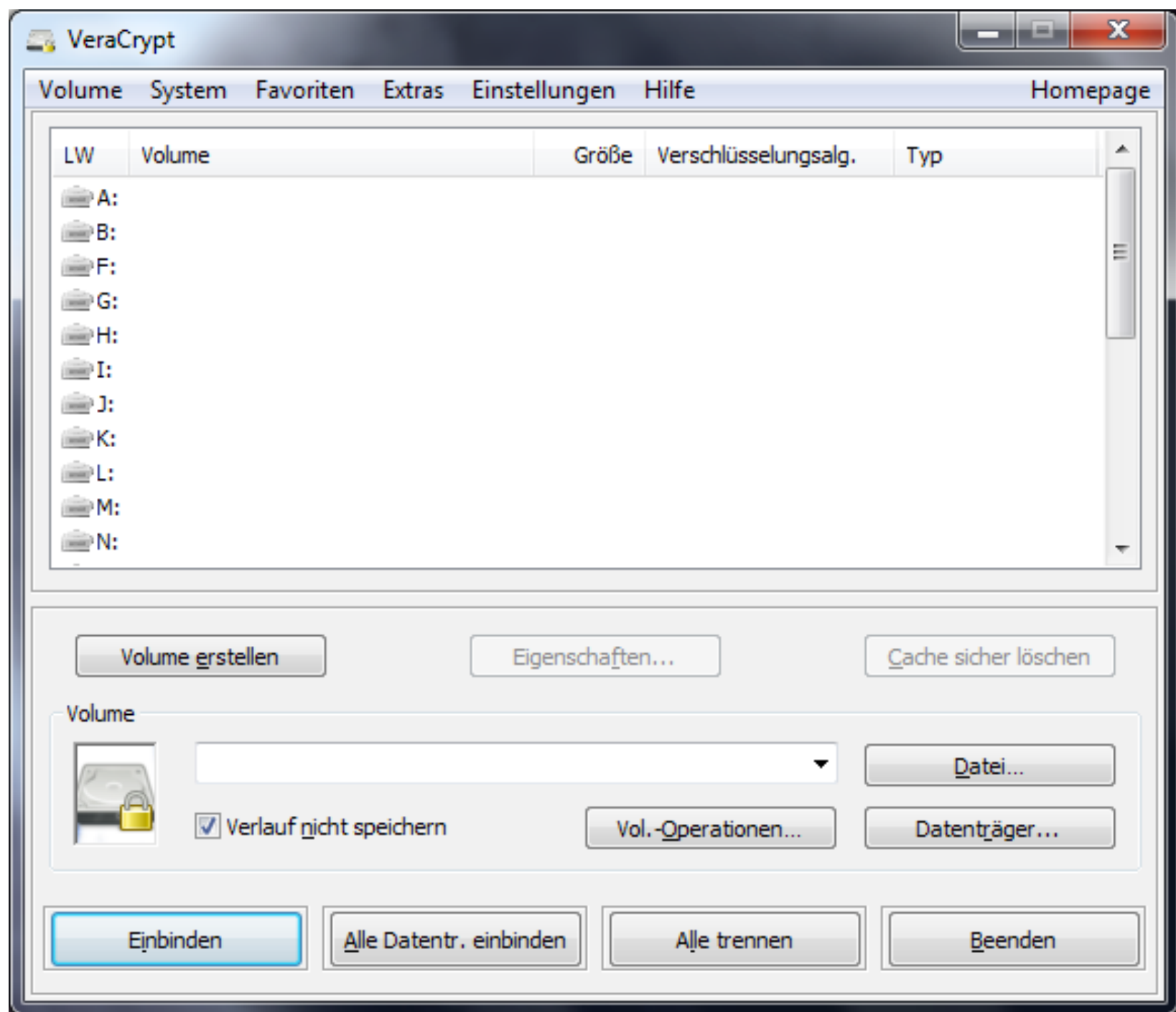


- Software: **VeraCrypt**
 - Software zur Dateiverschlüsselung
 - Quelloffen und auf allen gängigen Plattformen verfügbar
 - Freie Software
- Warum VeraCrypt?
 - Weil Windows-Verschlüsselung "BitLocker" vermutlich von Geheimdiensten geknackt werden kann

Über VeraCrypt (1)

Was kann ich mit VeraCrypt verschlüsseln?

- Container (verschlüsselte Ordner)
- Datenträger:
 - Festplatten/SSDs
 - CDs, DVDs... (Container)
 - USB-Sticks
 - ...
- Systempartition



Über VeraCrypt (2)

Vorteile

- Quelloffen, freie Software
- Nachvollziehbare Änderungen am Code
- Plattformübergreifend
- Auf USB-Stick transportierbar
- Unabhängiger Audit

Nachteile

- Komfortverlust
- Passwortverlust = Datenverlust

Umgang mit VeraCrypt

- Was will ich verschlüsseln?
 - Sicheres Passwort wählen
 - Adminrechte notwendig
 - Vorsicht bei fremden Geräten!
 - Generell: Benutzerhandbuch zu VeraCrypt lesen
- Größtes Sicherheitsrisiko ist fast immer der Nutzer!

Rechtliches

- Deutschland: Kein Zwang zur Herausgabe eines Passworts/Schlüssels bei möglicher Selbstbelastung
- Vorsicht im Ausland:
 - Großbritannien: Pflicht zur Herausgabe (→ RIPA), auch Beugehaft möglich!
 - USA: Ein- und Ausreise mit verschlüsselten Datenträgern problematisch

Tracking beim Browsen vermeiden & Tor

Datenschutzfreundliches Surfen mit Firefox

- „Das Web ist kaputt.“
- Auf fast allen Webseiten werden etliche Inhalte von Drittanbietern nachgeladen (nicht nur Werbung!)

Wie schrecklich ist die Web-Realität?

Beispiel: www.spiegel.de

Standard-Firefox, Debian 8 GNU/Linux

... so schrecklich!

Beispiel: www.spiegel.de

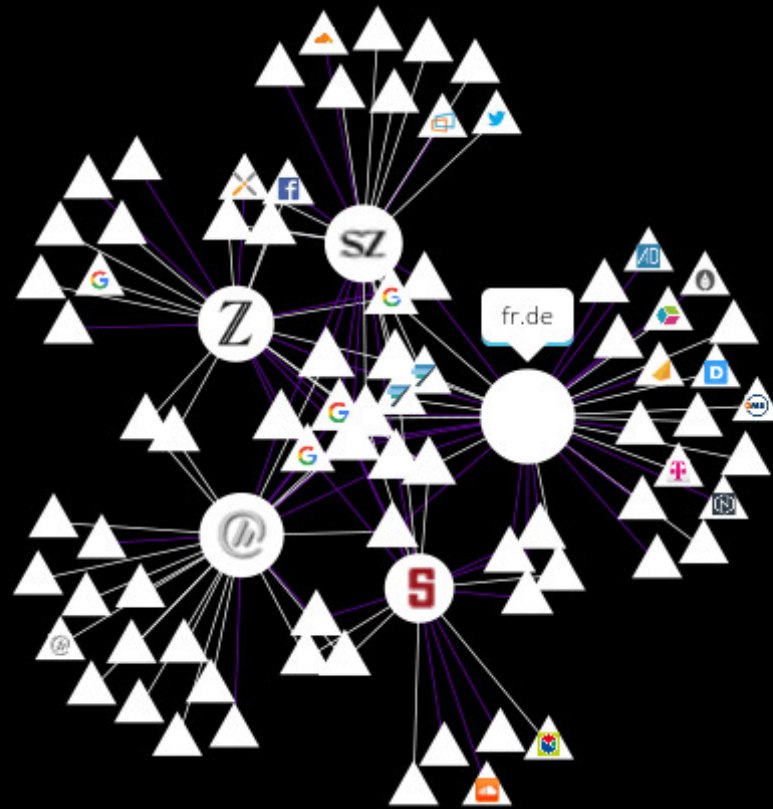
Standard-Firefox, Debian 8 GNU/Linux

- 136 HTTP-GETs an folgende Domains...
- spiegel.de, meetrics.net, ioam.de, adition.com, yieldlab.net, criteo.com, *flashtalking.com*, exactag.com, parsely.com, meetrics.net, outbrain.com, *atdmt.com*, *ligatus.com*, doubleclick.net, adform.net, google-analytics.com, *t4ft.de*, *westlottol.com*, *ligadx.com*, googlesyndication.com, *lqm.io*, *soundcloud.com*,
- 1,6 MB; 59 Cookies von 19 Domains
- Ladezeit ca. 17 Sek. (Core i5 M560)

Analyse im Firefox mit Lightbeam

DATA GATHERED SINCE MAY 24, 2017
YOU HAVE VISITED 7 SITES
YOU HAVE CONNECTED WITH 150 THIRD PARTY SITES

Daily
GRAPH VIEW



TOGGLE CONTROLS

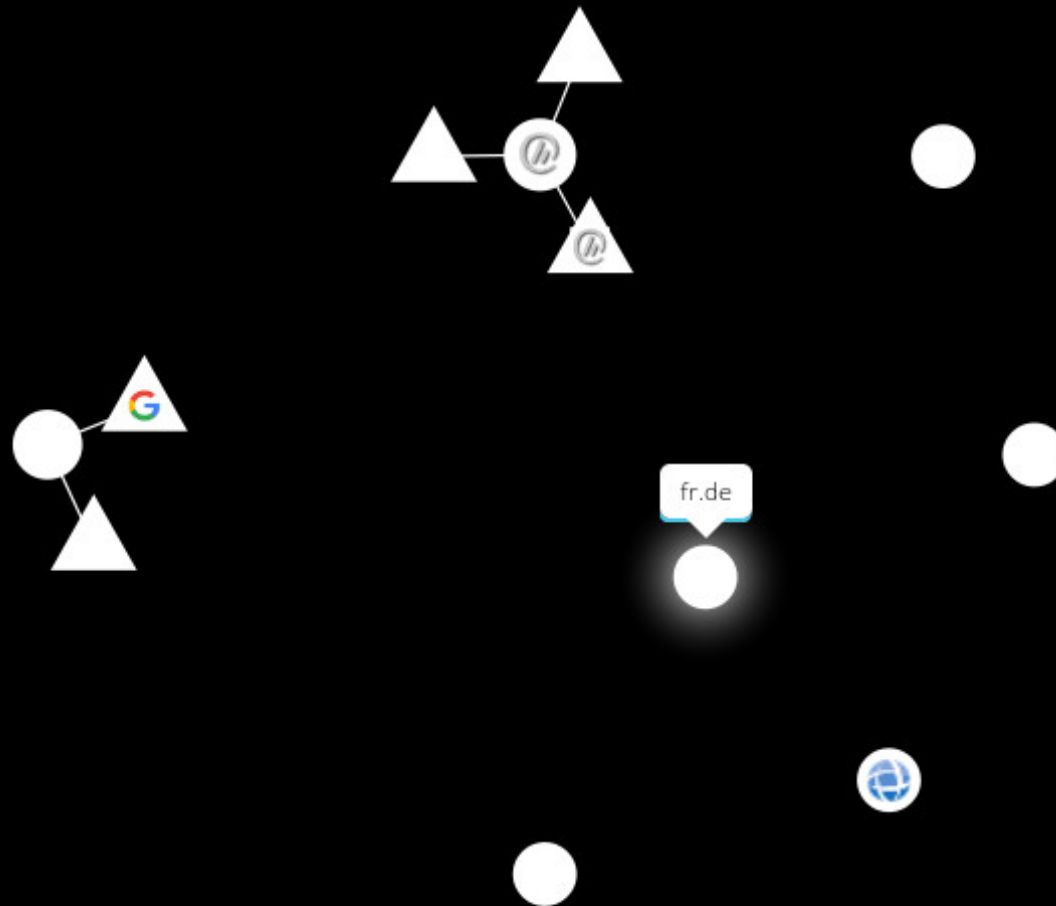
FILTER



Analyse im Firefox mit Lightbeam

DATA GATHERED SINCE MAY 24, 2017
YOU HAVE VISITED 7 SITES
YOU HAVE CONNECTED WITH 5 THIRD PARTY SITES


Daily
GRAPH VIEW




TOGGLE CONTROLS


FILTER

Einfach selber Testen mit Webbkoll

 webbkoll | dataskydd.net

FAQTech

 Svenska

http://www.example.com/ 

How privacy-friendly is your site?

Check

This tool helps you check what data-protecting measures a site has taken to help you exercise control over your privacy. [Read more.](#)

*Please note that this service is still under development. Some sites (sometimes) don't work; sometimes results are incorrect. We're working on it! **Also note** that the backend is currently running on only one server with very limited resources, so in case of usage spikes, waiting times can be long. (But you can [run your own instance!](#)) [Feedback](#) is appreciated.*

<https://webbkoll.dataskydd.net/en>

Wie kann ich mich vor Tracking schützen?

- Browser-Wahl
 - Firefox
- Browser-Einstellungen
 - Do-not-Track Option
 - Benutzerdefinierte Chronik:
Cookies (für Drittanbieter) deaktivieren
- Suchmaschinen
 - startpage.com, ixquick.eu, DuckDuckGo.com, MetaGer.de, etc.
(im Gegensatz zu Google auch keine individuellen Ergebnisse)
- Browser-Add-ons! ...

Firefox-Add-ons

- Tracker und Werbung blocken: **uBlock origin**
- Aktive Inhalte blocken: **NoScript**
 - Scripts Globally Allowed (vom Hersteller nicht empfohlen)
- Webseiten immer verschlüsseln: **HTTPS Everywhere**
- Cookies automatisch löschen: **Cookie AutoDelete**
- Adobe-Flash am besten entfernen oder deaktivieren!

Etwas komplizierter und aufwendiger:

- Alle Skripte blocken: **NoScript**
- Alle Drittanbieteranfragen blocken: **uMatrix**

Weitere Firefox-Funktionen

Privater Modus

- Keine **lokale** Speicherung von Daten besuchter Webseiten (insb. keine Chronik, keine URL-Vervollständigung, Cookies, etc.)
- Auf dem verwendeten PC verbleiben keine Spuren
- *Keine Anonymität* gegenüber dem Netz



Sie surfen im privaten Modus

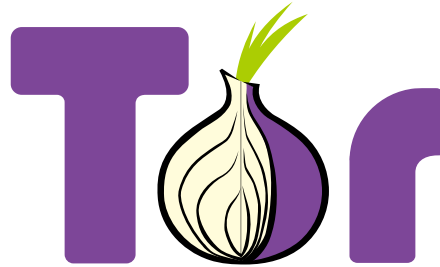
WebRTC (statt Skype)

- Firefox, Opera und Google Chrome
- Video-Telefonie **ohne Anmeldung**
- Aufbau durch Öffnen eines Links
- **Ende-zu-Ende-Verschlüsselung** mit **PFS**
- Keine starke Anonymität
- Läuft in der Amazon-Cloud
- Freie Software; eigenes Hosting möglich!

<https://meet.jit.si/>

Anonym surfen mit dem Tor-Browser

Tor (von „The Onion Router“)



Was ist Tor?

- Netzwerk zur Anonymisierung von Verbindungsdaten
- IP-Adresse wird verschleiert

Vorteile

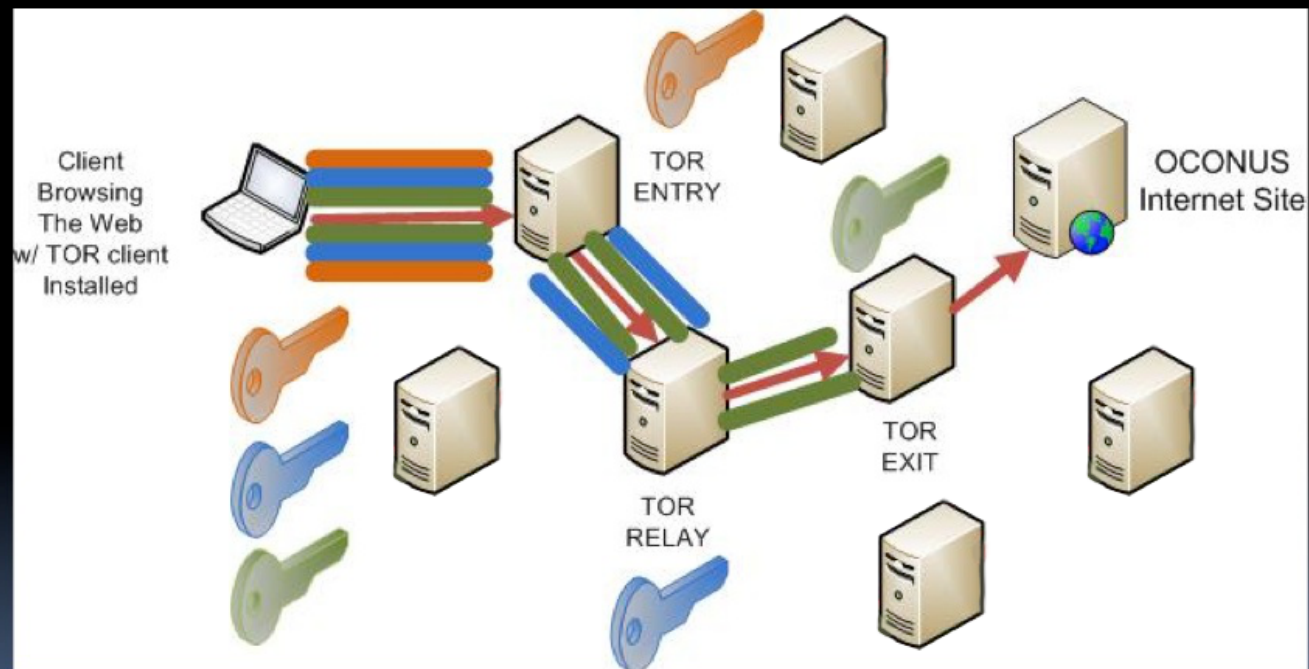
- Freie Software
- Anonymes Surfen

Nachteile

- Login bei personalisierten Seiten nicht sinnvoll
- Latenz ist größer



(U) What is TOR?

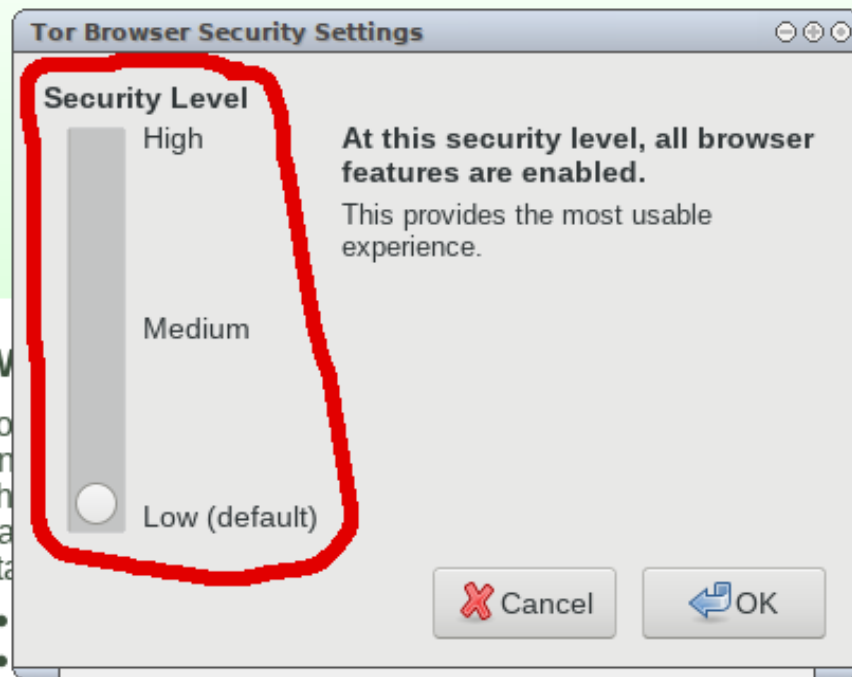




Welcome to Tor Browser

You are now free to browse the Internet anonymously.

[Test Tor Network Settings](#)



You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- [Run a Tor Relay Node »](#)
- [Volunteer Your Services »](#)
- [Make a Donation »](#)

Installation

<https://www.torproject.org/projects/torbrowser.html>

Mobilgeräte

Überwachung

- Geheimdienste sammeln
 - tägl. rund 5 Milliarden Standortdaten von Mobiltelefonen
 - tägl. Fast 200 Millionen SMS

Überwachung

...und werten sie unter bestimmten Blickwinkeln aus
(Kontaktbeziehungen, Reisedaten, Finanztransfers, ...)

...bzw. setzen die gesammelten Daten gezielt ein
(z. B. in der Ukraine Anfang 2014. SMS an Teilnehmer
einer Demonstration:

"Sehr geehrter Kunde, sie sind als Teilnehmer eines
Aufruhrs registriert.")

App-Berechtigungen: Facebook (1)

- Geräte- & App-Verlauf
 - Aktive Apps abrufen
- Identität
 - Konten auf dem Gerät suchen
 - Konten hinzufügen oder entfernen
 - Kontaktkarten lesen
- Kalender
 - Kalendertermine sowie vertrauliche Informationen lesen
 - Ohne Wissen der Eigentümer Kalendertermine hinzufügen oder ändern und E-Mails an Gäste senden
- Kontakte
 - Konten auf dem Gerät suchen
 - Kontakte lesen
 - Kontakte ändern

App-Berechtigungen: Facebook (2)

- Standort
 - Ungefährer Standort (netzwerkbasiert)
 - Genauer Standort (GPS- und netzwerkbasiert)
- SMS
 - SMS oder MMS lesen
- Telefon
 - Telefonnummern direkt anrufen
- Anrufliste lesen
 - Telefonstatus und Identität abrufen
 - Anrufliste bearbeiten
- Fotos/Medien/Dateien
 - USB-Speicherinhalte lesen
 - USB-Speicherinhalte ändern oder löschen
- Speicher
 - USB-Speicherinhalte lesen
 - USB-Speicherinhalte ändern oder löschen

App-Berechtigungen: Facebook (3)

- Kamera
 - Bilder und Videos aufzeichnen
- Mikrofon
 - Ton aufzeichnen
- WLAN-Verbindungsinformationen
 - WLAN-Verbindungen abrufen
- Geräte-ID & Anrufinformationen
 - Telefonstatus und Identität

App-Berechtigungen: Facebook (4)

- Sonstige
 - Dateien ohne Benachrichtigung herunterladen
 - Größe des Hintergrundbildes anpassen
 - Daten aus dem Internet abrufen
 - Netzwerkverbindungen abrufen
 - Konten erstellen und Passwörter festlegen
 - Akkudaten lesen
 - dauerhaften Broadcast senden
 - Netzwerkkonnektivität ändern
 - WLAN-Verbindungen herstellen und trennen
 - Statusleiste ein-/ausblenden
 - Zugriff auf alle Netzwerke
 - Audio-Einstellungen ändern
 - Synchronisierungseinstellungen lesen
 - Beim Start ausführen
 - Aktive Apps neu ordnen
 - Hintergrund festlegen
 - Über anderen Apps einblenden
 - Vibrationsalarm steuern
 - Ruhezustand deaktivieren
 - Synchronisierung aktivieren oder deaktivieren
 - Verknüpfungen installieren
 - Google-Servicekonfiguration lesen

App-Berechtigungen

- Sich selbst die immer Frage stellen, ob Apps bestimmte Berechtigungen für ihre Funktion benötigen.
- Einzelne Berechtigungen von Apps entziehen.
- Alternative Apps nutzen, die weniger Berechtigungen benötigen.
- Falls verfügbar: Datenschutzmodus aktivieren!

Smartphones & Tablets

- Hardware („Super-Wanze“)
 - Mikrofon, Kamera, GPS, Bewegungssensor
- Betriebssystem
 - iOS (Apple) oder Windows Phone/Mobile (Microsoft)
= Pest oder Cholera
 - Apps nur aus einer Quelle (zentraler App-Store)
 - Geschlossene Systeme, keine Gerätehoheit
 - Mehr Freiheit durch Jailbreak (Gefängnisausbruch)

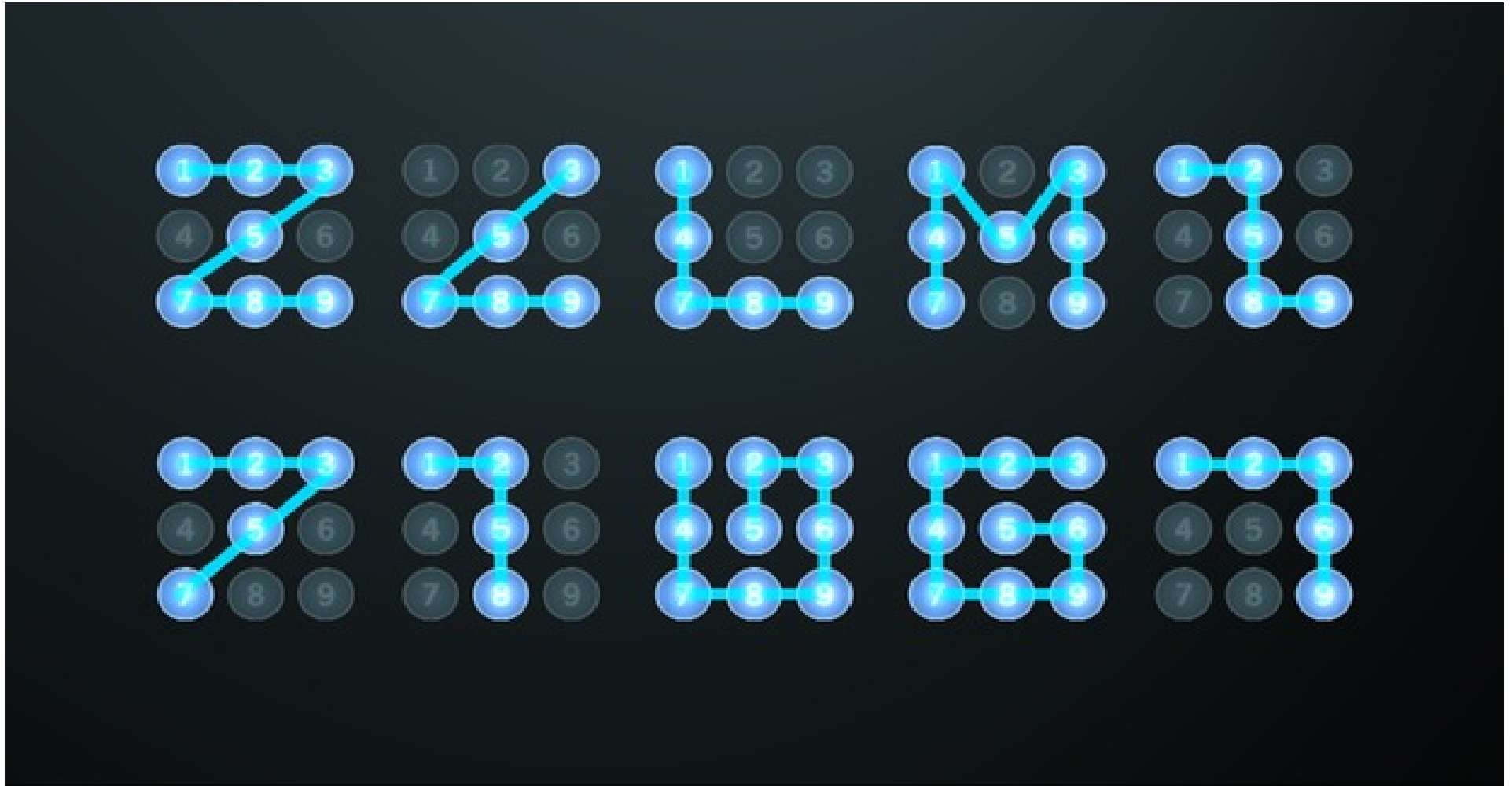
Android

- Theoretisch gute Basis
 - Linux-basiert, Freie Software
- **Aber:** tiefe Integration proprietärer Google-Software
 - Suche, Browser, Gmail, Maps, Kalender- / Kontakte-Sync ...
 - Play Store & Google-Dienste
 - Fernzugriff, Datenübermittlung
 - standardmäßig keine Gerätehoheit
 - Je nach Hersteller oft nur zwei Jahre lang Sicherheitsupdates

Erste Schritte: Konfiguration

- Sichere Bildschirmsperre
 - von unsicher zu sicherer:
Wischgeste, Muster, Biometrisch, PIN, Passwort
- Speicher verschlüsseln
- WLAN, GPS, Bluetooth, etc. ausschalten, wenn nicht genutzt
- Browser (Firefox) gegen Tracking schützen

Typische Wischgesten



Android ,entgoogeln‘

1. Unnötiges entfernen

- Google-Einstellungen (G+, Standort, Suche, Werbe-ID, usw.)

2. Alternativ-Dienste nutzen

- Browser, Suche, Mail, Sync für Kalender / Kontakte...

3. Play Store löschen / **F-Droid nutzen**

- App-Alternativen nutzen

4. Freie Android-Variante installieren

- z.B. LineageOS, Replicant

Ansprüche an Messenger

- Für alle gängigen Betriebssysteme verfügbar
- Ende-zu-Ende-Verschlüsselung
- Sicherer Verschlüsselungsalgorithmus (AES)
- Dezentralität / Möglichkeit für eigene Server
- Quelloffen (Überprüfung durch unabhängige Experten)
- Upload von Daten (z.B. Adressbuch) nur mit ausdrücklicher Bestätigung des Nutzers
 - Adressbuch enthält Daten anderer Personen → Upload erlaubt?
- Unabhängige Installation und Betrieb
 - z.B. ohne Google Play Store & Google-Dienste

Warum sollte ich einen anderen Messenger benutzen?

- Problem: Wer WhatsApp nutzt, gibt die Telefonnummern all seiner Kontakte automatisch an das Unternehmen weiter
- Verstoß gegen geltendes Recht: Zustimmung jedes(!) einzelnen Kontaktes notwendig!
- Urteil AG Bad Hersfeld: Mutter muss schriftliche Einwilligung von jedem Kontakt im Smartphone-Adressbuch des Sohnes einholen
- Zum Nachlesen AG Bad Hersfeld (Urt. v. 20.03.2017, Az. F 111/17 EASO)

Messenger-Vergleich

	Signal	Telegram	Surespot	Threema	WhatsApp
Freie Software	ja	teils	ja	nein	nein
Ende-zu-Ende-Verschlüsselung	ja	(ja)	ja	(ja)	(ja)
unabhängiges Audit	ja	ja	nein	(ja)	nein
Adressbuch-Zugriff	ja	ja	nein	(nein)	(nein)
Nicknames (Pseudonyme)	nein	nein	ja	ja	nein
außerhalb Play-Store erhältlich	ja	ja	nein	ja	ja
funktioniert ohne Google-Dienste	ja	ja	nein	ja	nein
Verbreitung	mittel	weit	kaum	mittel	sehr weit

Links & Literatur

PRISM Break zu Android & iOS

- <https://prism-break.org/de/categories/android/>
- <https://prism-break.org/de/categories/ios/>

Mike Kuketz: Your phone Your data – Android ohne Google?!

- <https://www.kuketz-blog.de/your-phone-your-data-teil1/>

Digitalcourage: Digitale Selbstverteidigung

- <https://digitalcourage.de/digitale-selbstverteidigung/mobil>

Weitere Projekte

- **PRISM Break:** (<https://prism-break.org/de/all/>)
Liste datenschutzfreundlicher Software und Anbieter, z.B.:
 - *Startpage* und *DuckDuckGo* statt Google-Suche
 - *OpenStreetMap* statt Google Maps
 - *Dudle* statt doodle
 - *EtherCalc* und *EtherPad* statt Google Docs
 - *Diaspora** statt facebook oder Google+
 - ...
- **Digitalcourage: Digitale Selbstverteidigung**
(<https://digitalcourage.de/digitale-selbstverteidigung>)
 - Übersichts-Flyer hier im Raum zum Mitnehmen!

Kontakt & Termine

E-Mail: digitalcourage.hsg@uni-bielefeld.de

Key-ID: B1CB6584

Fingerprint: 2DD5 1926 5447 EB1C 78E1 8734 A279 303B B1CB 6584

Web: <https://digitalcourage.de/hsg>

Besucht uns — Treffen der HSG:

1. und 3. Montag im Monat, 18 Uhr im SozCafé (X-C2-116)